Electricity Infrastructure Enhancement for the Security of Supply against Coordinated Malicious Attacks

Electricity Infrastructure Enhancement for the Security of Supply against Coordinated Malicious Attacks

Abouzar Estebsari, Tao Huang, Enrico Pons, Ettore Bompard
Dipartimento Energia
Politecnico di Torino
Turin, Italy
abouzar.estebsari@polito.it, tao.huang@polito.it, enrico.pons@polito.it, ettore.bompard@polito.it

***Abstract*— The impact of coordinated malicious attacks may be dramatically severe and may yield a wide area blackout. A preventive measure is enhancing the infrastructure through investment. Due to limited budget, a decision making is required to select the best possible options, considering cost/benefit ratio. We designed a time-step simulation framework representing the evolution of post-contingency failures and load/system restoration. System unserved energy is translated into economic losses. Different enhancement options can be compared in terms of benefit (reduction in the cost of unserved energy) and of cost (investments needed) to eventually rank them. The simulation framework also provides a way to derive an optimal lost load recovering strategy to accelerate system restoration. In this paper the simulation framework is applied to a real network (Austrian transmission grid) to evaluate the technical and economic impacts of a coordinated malicious attack.**

Keywords*— *Malicious threats, Cost benefit analysis, Power System Security, Time-Step Simulation, Transmission Infrastructure Enhancement.

I. INTRODUCTION

With the extensive growth of malicious activities, power systems, as key critical infrastructures, are attracting terrorists' attention. The impact may be dramatically severe and may yield more frequent blackouts [1]. In recent years, malicious attacks started to occur and a growing trend has been observed. Malicious threats to power systems can be originated by intentional actions from different agents (terrorists, criminal groups, cyber attackers, copper thieves, vandals, psychotics, malware writers, etc.) by various means (explosives, high power rifles, malware, etc.) with the willingness to cause damage for personal, political, or economic benefits. From 1999 to 2002, there were more than 150 deliberate attacks to power systems around the world [2]. Since September 11, 2001, efforts to prevent and protect power systems against growing malicious threats had a sudden increase with international security concerns [3]. Modelling and simulation of malicious attacks to power systems is becoming a hot area of research nowadays [4].

Malicious attacks, by incapacitating or destructing power systems may have a debilitating impact on many different society sectors like health, safety, security and economy. Power systems consist of three layers: a physical layer including the network infrastructure components like power plants, transmission lines, transformers, etc. and also physical equipment supporting information flows and communication system; a human layer including both the employees to be protected and the personnel who may present an insider threat (e.g., due to privileged access to control systems, operations, and sensitive area and information); and a cyber layer, including the communication network and information system which serve the functioning and operation of electric power system, which takes a critical role in control, dispatching, and other operational affairs.

A malicious threat can trigger an initiating event on/through anyone of the above three layers to cause harm to the power system or induce it to fail. According to the three layers of power systems, malicious threats can be classified into physical threats, human threats, and cyber threats [5], [6]. Malicious attacks through physical layer can be sub-divided into terrorist attacks [7], war acts and sabotage. They are intentional destructive actions which intend to cause massive blackouts by destroying one or more components of a power system/network (substation, power plant, power unit, line, control center, transmission site, IT system, etc.) with direct damage on them, affecting the normal operation of the system. Human threats refer to the intentional operators' intervention to cause problems for the normal functionality of the system especially on the most vulnerable points, which may be clearly identified for them. Malicious cyber threats can be divided into two types with respect to the attack procedure as malware and hacking, and are triggered by unauthorized access users who exploit the vulnerabilities of the power system cyber layer.

The mechanism of these threats shows that the variety of the targets in power systems to be attacked is huge. Depending on the purposes of attackers, different parts of the system will be affected. The targets being attacked by initiates are usually chosen carefully and deliberately. Attackers with the willingness of causing massive blackouts will actively exploit system vulnerabilities to plot attack strategies in terms of when, how and where. The main challenge in achieving a desired security level is in using the resources in the best possible way [8]. Different budget allocation will obviously shape the shield against malicious attacks, yet we cannot shield them all at the

This paper has been produced with the financial assistance of the SESAME project (a FP7-security project co-funded by the European Commission with grant number 261696, aiming at providing a contribution to the development of tools and a regulation framework for the security of the European power grid against natural, accidental and malicious attacks.

same level. This implies some kind of decision making, whose objective is to ensure the ability of the system to withstand some level of impacts from threats, by means of the enhancement of the infrastructure, with the best cost-benefit ratio. Preventive measures based on infrastructure enhancement consist of an extension of the available resources in the network, anticipating investments, which would not be necessary at this time, but which can secure the system against future potential coordinated attacks. This makes the network ready to lose some of its elements while keeping most of its performance.

Different approaches already exist in literature for evaluating and modelling the resilience, reliability and security of power systems when subject to natural (extreme weather conditions) or malicious incumbent threats [11], [12], [13].

We designed a time-step simulation framework to chronologically simulate the system behavior after the occurrence of a contingency which initiates cascading failures [9], including automatic responses from existing protection schemes and human-driven operational strategies. The algorithm also provides a way to derive an optimal lost load recovering strategy (aiming at minimizing load shedding and maximizing load pick up) to accelerate the restoration of lost load. This simulation tool fits and serves in a proposed cost-benefit analysis framework [14].

In the next section, the developed simulation framework will be briefly introduced. In section III we describe a decision making procedure based on cost-benefit analysis. We apply then the simulation framework to a real network (the Austrian transmission grid) as a study case to evaluate the technical and economic impacts of a coordinated malicious attack. The impacts of the attack will be compared between two cases: in the existing network without enhancement and in the reinforced system. The results are presented in section IV, where a cost-benefit analysis of the enhancement of the infrastructure to secure the Austrian power system against malicious attacks is also discussed.

II. SIMULATION FRAMEWORK

We developed a simulation framework to model the system behavior after the occurrence of a contingency; it provides system status snapshots for a predefined set of discrete time points. The system status includes both technical (e.g. bus voltages, element operational status, line flows, etc.) and economic (e.g. operational cost and unserved energy) information. An algorithm for making optimal decision of load/system restoration is taking into account load shedding minimization and load pick up maximization. This tool is designed to identify the most effective counteractions to reduce the vulnerability and provides a basis for economic evaluation of threats [15].

The tool carries out a fully integrated simulation considering: events that take place on the network (called “triggering events” like a generator trip), impacts (like unserved energy), and effectiveness of the protective measures (like damage cost reduction due to the addition of a new line to the network).

The simulation tool structure includes three main modules: *time control*, *system automatic response* and *optimal operation decision* modules. The *time control* module schedules the sequence of functions and models automatic restoration of system elements (e.g. lines reclosure), operator interventions (e.g. manual load shedding), and load profile following (Fig. 1).

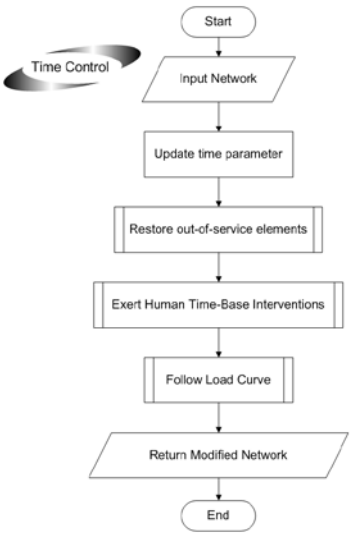

Fig. 1 High level flowchart of time function for simulation scheduling

In the *system automatic response* module (Fig. 2), existing protection schemes (e.g. frequency and voltage control [16]) are modeled. As the main purpose of the study is to assess blackout impacts, to eventually evaluate and rank the effective countermeasures (especially long term plans of infrastructure enhancement), the simulation observation windows are hardly less than a minute. These sample times are predefined by the user to create a sequence of time-points in which system status snapshots could be represented. Human-driven restoration strategies cannot take place as fast as system automatic response: for this reason another time factor is introduced by the user to set the initial time of the restoration process and optimal decisions.

Cascading failures may cause separation of a portion of the grid as an island. The designed simulation tool can handle islanding considering both automatic responses and restoration plans. If an island is in blackout, during restoration, a designed black-start algorithm re-energizes the island if possible (based on available resources considering load prioritization). Islands can also get integrated again if interconnection lines are reclosed and the feasibility check module permits.

As shown in Fig. 3, these restoration and integration schemes are all modeled in a module called *optimal operation decision* where a three step load restoration strategy is also applied. For each bus connected to loads, the user can introduce interruptible portion and sheddable loads. Sheddable load can be defined according to the regulations: for example, ENTSO-E sets 50% of loads as a sheddable portion during under frequency load shedding. Interruptible loads are considered as the lowest prioritized loads whose disconnection would cost less. A 3-step strategy is applied to find a feasible solution with the objective of minimum load shedding and

maximum restoration: S1 - restores all prioritized loads and tries to restore as much as possible the rest; S2 - restores all the non-sheddable loads and tries to restore as much as possible prioritized loads; S3 - restores as much as possible loads regardless of their priorities.

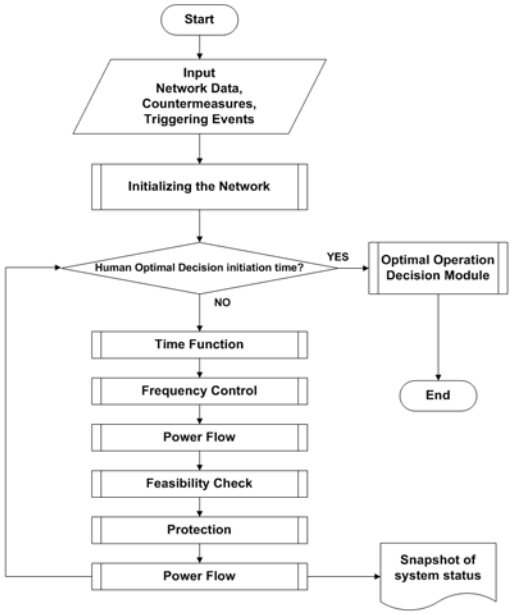

Fig. 2 High level flowchart of system automatic response

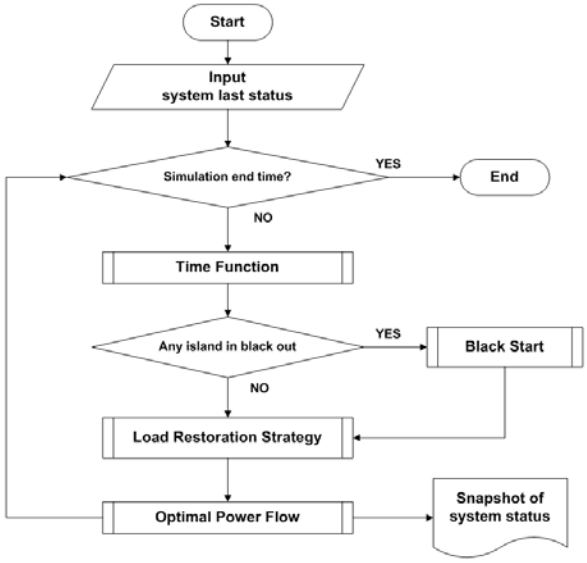

Fig. 3 High level flowchart of restoration optimal decision module

The simulation results contain, for each system operational status, information on all network elements status (bus, branch, and generators), extra operational cost (the additional cost due to the adjustment of the generator and load power to mitigate the cascading effects of the triggering events), investment cost, unserved energy, etc. The outcome of the calculation core is used to generate maps/graphs of network topology containing operational status of components to replay the post-contingency evolution. The developed algorithm is implemented in MATLAB® and compiled to build a stand-alone software for post-contingency simulation of large-scale power systems, such as the European power transmission grid.

III. DECISION MAKING BASED ON COST-BENEFIT ANALYSIS

During the cascading failures initiated by a contingency, some loads may not be supplied and system may experience some amount of unserved energy. This can be translated into economic losses by taking into account the unserved energy cost. To reduce this cost, different protection schemes or investment options can be considered, but as these countermeasures would also introduce some costs, they have to be compared through a cost-benefit analysis in advance.

The key components to make decisions are summarized in the framework shown in Fig. 4. Due to budget limits to deploy new countermeasures for enhancement, a decision making is required to select the best possible options, considering cost/benefit ratio. We developed a time-step simulation tool to model the physical network and emulate system behavior after contingencies occur. From a list of most imminent threats collected in what we called "Threat Catalogue", and the information from "Vulnerability Identification" which contains the list of most critical elements, affected network components can be defined as an input to the simulation tool. Enhancement options as "Countermeasures" are the other input to the network simulation tool. Different enhancement options can be compared in terms of benefit (reduction in the cost of unserved energy) and of cost (investments needed) to eventually rank them. The threat risk can be also ranked by comparing different threats along with corresponding countermeasures. In the following discussions, we briefly introduce the calculation framework to achieve this goal.

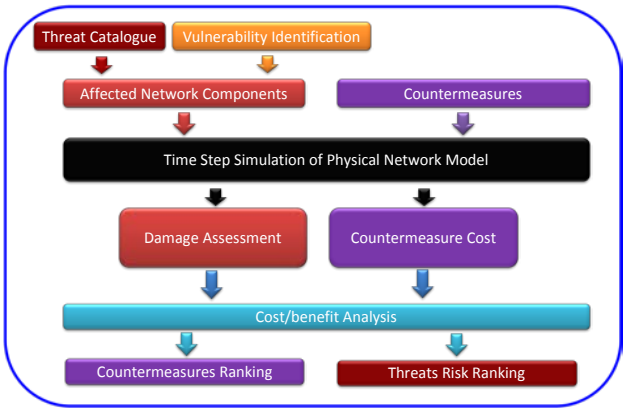

Fig. 4 Framework of the Decision Support System key components

A. *Calculation framework for cost-benefit analysis*

As described before, to perform a cost-benefit analysis, the two components of damage assessment and countermeasure cost are needed (Fig. 4). The total blackout cost depends on the extra operational cost and economic loss to the society. To evaluate physical damages, we need to calculate extra operational cost and unserved energy cost. Extra operational cost is the added-up cost due to the adjustment in the generator and load to mitigate the effects of the triggering events. Extra operational cost sources are coded as set O (1) where *i* represents the source and gets 2 different IDs: "1" for generator extra operational cost, and "2" for load extra operational cost.

$$i \in O, \quad O = \{1,2\} \tag{1}$$

Considering set S for the scenarios IDs, CG for the countermeasure group IDs, L for the loss events IDs, G for the generator IDs and set D for demands IDs (loads), the following assumptions are made:

$$j \in S \quad S = \{1,2,...,n_S\}, S \subset \mathbb{N} \tag{2}$$

$$k \in CG \quad CG = \{0,1,2,...,n_{CG}\}, CG \subset \mathbb{N}^0 \tag{3}$$

$$l \in L \quad L = \{1,2,...,n_L\}, L \subset \mathbb{N} \tag{4}$$

$$g \in G \quad G = \{1,2,...,n_G\}, G \subset \mathbb{N} \tag{5}$$

$$d \in D \quad D = \{1,2,...,n_D\}, D \subset \mathbb{N} \tag{6}$$

The set CG in (3) contains 0 to include the case without any countermeasures, i.e. the baseline for comparing the effects of applied countermeasures out of set CG.

The main cost of frequency control is from the extra payment to the generator and load for compensating the deviation from their scheduled value. Supposing in the time interval t, generator g was ordered to change its output from $P_g(t_1)$ to $P_g(t_1+t)$, the extra operational cost for frequency control for scenario j, countermeasure group k and loss event l, is $C(i,j,k,l)$ where $i=1$. Assuming R_g as the reserve of generator g, C_{Rg} as the cost of reserved power of generator g, and C_g as the operational cost of generator g, (7) represents how we calculate generator extra operational cost.

$$C(1,j,k,l) = \begin{cases} \sum_{g=1}^{n_G} (C_{R_g} \mid P_g(t_1+t) - P_g(t_1) \mid t) \\ \qquad if \mid P_g(t_1+t) - P_g(t_1) \mid < R_g, \\ \sum_{g=1}^{n_G} (C_{R_g} R_g t + C_g(\mid P_g(t_1+t) - P_g(t_1) \mid - R_g)t) \\ \qquad if \mid P_g(t_1+t) - P_g(t_1) \mid \geq R_g. \end{cases} \tag{7}$$

Supposing, load d was ordered to change its consumption from $P_d(t_1)$ to $P_d(t_1+t)$, the extra operational cost of the loads for frequency control for scenario j, countermeasure group k and loss event l, is $C(i,j,k,l)$ where $i=2$. (8) represents how we calculate load extra operational cost.

$$C(2,j,k,l) = \begin{cases} \sum_{d=1}^{n_D} (C_d^{\text{int}} \mid P_d(t_1+t) - P_d(t_1) \mid t) \\ \qquad if \mid P_d(t_1+t) - P_d(t_1) \mid \leq I_d, \\ \sum_{d=1}^{n_D} (C_d^{\text{int}} I_d t + C_d^{shed}(\mid P_d(t_1+t) - P_d(t_1) - I_d \mid)t) \\ \qquad if \ I_d < \mid P_d(t_1+t) - P_d(t_1) \mid \leq S_d, \\ \sum_{d=1}^{n_D} (C_d^{\text{int}} I_d t + C_d^{shed}(S_d - I_d)t \\ + C_d^{nshed}(\mid P_d(t_1+t) - P_d(t_1) - S_d \mid)t) \\ \qquad if \mid P_d(t_1+t) - P_d(t_1) \mid > S_d. \end{cases} \tag{8}$$

Where C^{int}_d, C^{shed}_d and C^{nshed}_d are the prices for interruptible load, sheddable load and non-sheddable loads; I_d and S_d are maximum for the interruptible load and the sheddable load.

In the restoration phase, if the generator output changes with respect to the operational point, the extra operational cost is calculated as it is described in the frequency control countermeasure part. If the generator is off and the black start is being taken into account in the restoration phase, the extra operational cost is also calculated but considering the black start service cost.

Countermeasure cost in Fig. 4 refers to the long-term investment for infrastructure enhancement. Considering set E as the set of invested elements under countermeasure group k, the total investment cost would be calculated as (10).

$$e \in E_k \quad E_k = \{1,2,...,n_{E_k}\}, E_k \subset \mathbb{N} \tag{9}$$

$$C^{inv}(j,k,l) = \sum_{e=1}^{n_E} \left(\frac{C_e^{init}(j,k,l)}{D_e(j,k,l)} + C_e^{Per}(j,k,l)\right) \tag{10}$$

Where C^{inv} is total investment cost, C^{init}_e is initial investing cost of installation element e, D_e is depreciation year of the installation element e, and C^{per}_e is the periodical cost of installation element e per year.

Supposing the total blackout cost (including extra operational cost and social cost) for scenario j, and loss event l, without any countermeasures to be evaluated is $C_T(j,k,l)$ where $k=0$, and the total blackout cost under the same scenario and the same loss event with countermeasure k is $C_T(j,k,l)$, then:

$$C_M(j,k,l) = C_T(j,0,l) - C_T(j,k,l) \tag{12}$$

$$B(j,k,l) = C_M(j,k,l) - C^{inv}(j,k,l) \tag{13}$$

where $C_M(j,k,l)$ is the reduced monetary loss of blackout under the same scenario with and without a specific countermeasure k, which signifies the impact on the level of the security of supply for the evaluated countermeasure k; $B(j,k,l)$ is the gain of applying countermeasure k.

After the calculation of all countermeasures under study over a reasonable set of scenarios, we can rank the impacts of different countermeasures on the level of security according to the $C_M(j,k,l)$, as well as selecting the highest cost-benefit countermeasures by ranking $B(j,k,l)$.

IV. CASE STUDY

In this section, we introduce an example of application of the described tool for a cost-benefit analysis of infrastructure enhancement for the Austrian transmission system. The original data of the Austrian transmission system (extracted from Qiong Zhou and Janusz W. Bialek's model of the European interconnected system [10]) was modified to ensure the n-1 contingency compliance for the load flow. Tie-lines are modeled with equivalent generators assigned to the buses geographically located in the neighboring countries. The capacity of each generator is set according to the capacity of the tie lines. The total generation capacity of the system is 19400 MW and 16920 Mvar. The simplified model of the system has totally 14 generators representing neighboring buses as equivalent generators, and 25 generators located inside Austria. 114 transmission lines exist in this model connecting

49 buses. There are 19 loads with initial total consumption of 6793 MW and 1888.5 Mvar.

The benefits of adding two new lines (Fig. 5) are analyzed and compared with the base case in terms of unserved energy. This network enhancement was suggested by the Austrian Regulator (E-Control) based on their experience and on a vulnerability analysis of the network elements. The sequence of post-contingency failures ("cascading failure") and the restoration actions over time is simulated for a total duration of 500 minutes (over 8 hours).

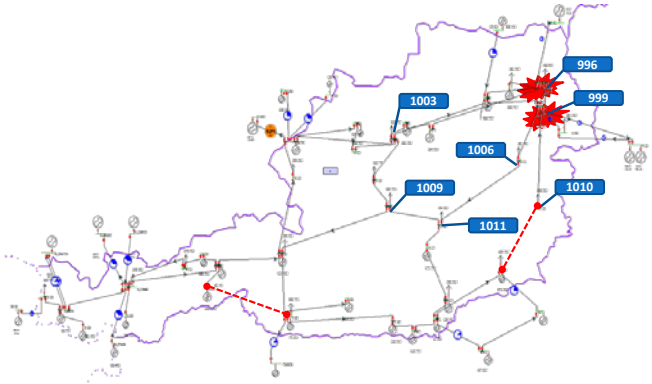

Fig. 5 Triggering events destroy 2 buses - 2 additional lines are studied as long-term countermeasures

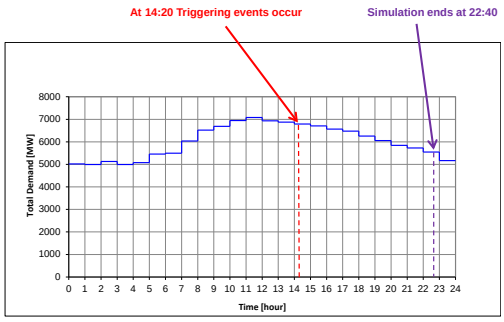

Fig. 6 Assumed load curve for the Austrian case

The threat scenario is characterized by a coordinated terrorist attack which causes the failure of two big substations (bus 996 and 999) near Vienna (Fig. 5). The two substations are assumed to be out of service for the whole study period (the 500 minutes). This kind of attacks requires the coordination of different people (groups) to be carried out. Therefore, the probability (events/year) would be lower than other events without this level of coordination/preparedness in advance. However in case of occurrence, the impact on the society can be huge. Vienna in fact is the capital and largest city of Austria. It has a population of around 1.7 million people, 2.4 million people within its metropolitan area (more than 20% of the Austrian population). With the same procedure explained in the previous section, investment benefits of adding two new transmission lines aiming at mitigating the impacts of power outage can be studied.

Considering the time points set for the time function (every 3 minutes for the automatic response iterations, every 45 minutes for capturing the optimal operation decision snapshots, and 30 min as the initiating time of the optimal decision process) and the changes in the load (discretized 24-h load curve shown in Fig. 6) the simulation tool provides 21 different snapshots of the system in terms of frequency, bus voltages, line flows and congestions, generator operation status, islanding information, unserved energy in each load, etc.

As described before, evolution of snapshots would provide insights to the technical aspects of system status which are interesting for power system operators, but what would eventually play an important role in decision making of long-term infrastructure enhancement is the assessment of corresponding damage cost and economic losses. Therefore, in this example, we focus on the amount of total unserved energy in the two different cases, with and without new lines.

Fig. 7 represents the load shedding percentage of some buses with respect to the expected demand from the load profiles. Although loads 1009 and 1011 experience less interruptions in the case without the new lines, the blackout in bus 1010 during the whole studied time (8 hours) results in a large amount of unserved energy. On the contrary, in the case with the two new lines, bus 1010 is being continuously 100% supplied.

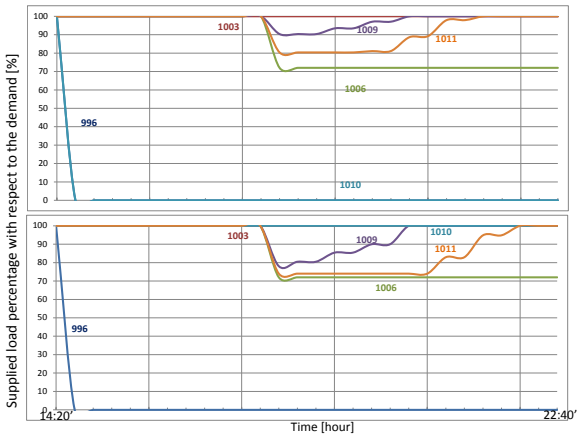

Fig. 7 Load shedding tracking – without and with adding new lines

Fig. 8 shows the last snapshot for the two cases. Thanks to one of the new lines, bus 1009 near Vienna with 308 MW load could be saved and served during the post-contingency evolution of the system, and that eventually resulted in a lower unserved energy in the case with countermeasures. The total unserved energy during the 500 minutes is 13631.5 MWh for the base case, and it is reduced to 11616.7 MWh in the case with the two additional lines. In order to monetize the impact of the new lines on the level of security of supply, the total costs should be compared. To calculate the cost of unserved energy, we use the simplified relation Cu= G/E in which Cu is the cost of unserved energy, G is the GDP and E is the domestic electricity consumption. In this simulation scenario, G and E values are taken from key statistics 2011 report of the Austrian regulator (E-Control) [17]. The calculated cost of unserved energy is Cu= 3800 €/MWh for year 2010. Therefore, the economic loss would be reduced from 51,799,700 € to 44,143,460 € with a saving of 7,656,240 € if the small amount of extra operational cost is neglected. This difference is actually the avoided cost thanks to the enhancement of the transmission system with two new lines. Comparing this avoided cost with the investment cost results in what we called

gain of applying the countermeasure. However, it should be noted that the study time window is 8 hours, in which a lot of large loads could not get restored in the case without additional lines. Therefore, the amount of unserved energy until the end of recovery process gets very high, which highlights the effectiveness of the new lines in the cost-benefit analysis.

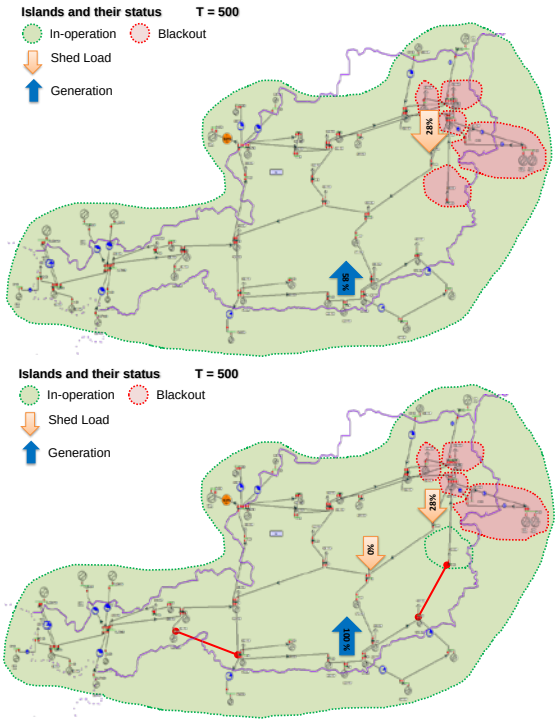

Fig. 8 Last snapshot – without and with invested lines

V. Conclusion

On one side threats to the electricity infrastructures security, especially malicious attacks are drawing increasing attentions due to their variety of targets and huge impacts. On the other side investment is needed for maintaining a certain level of security. Multiple options of infrastructure enhancement to secure the system against attacks need to be justified and selected before investing, due to limited budgets. In this paper, we applied a time step simulation tool with cost-benefit analysis capabilities to show how appropriate infrastructure enhancement could reduce attack impacts on power systems. As a case study, we designed a catastrophic scenario of malicious attack on the Austrian transmission network to evaluate the effectiveness of system structural reinforcement on unserved energy reduction. The simulation results of the case study show that adding two new lines to the system would reduce 15% of damage cost only from the point of view of unserved energy cost. The reduction in practice would be much higher: firstly because recovery process after occurrence of such a huge attack takes much longer than only 8 hours, which eventually results in a larger amount of unserved energy; secondly, because in the damage assessment, the economic loss is not calculated based only on the unserved energy cost, but also the monetized impacts of the outage on society is taken into account. Nevertheless, applying the developed framework, taking into account other options of infrastructure enhancement, could help decision makers to invest on the most appropriate choices. One of the added transmission lines has already been installed in the real network to enhance the level of security of transmission in Austria, and this can verify and validate the obtained results of this simulation framework.

References

[1] R. Zimmerman, C. Restrepo, J. Simonoff, L. Lave, “Risk and economic costs of a terrorist attack on the electric system,” in *CREATE economics of terrorism symposium*; 2005.

[2] S. Larsson and E. Ek, “The black-out in southern Sweden and eastern Denmark,” *IEEE*, September 23, 2003.

[3] The 9/11 commission, Final Report of the National Commission on Terrorist Attacks upon the United States. 2002. http://www.9-11commission.gov/report/index.htm.

[4] E. Bompard, , C. Gao, M. Masera, R. Napoli, A. Russo, F. Xue, and A. Stefanini, “Approaches to the Security Analysis of Power Systems Defence Strategies against Malicious Threats,” in Proc. *Luxembourg. Office for Official Pubb. of the European Communities*, 2007, p.1-51.

[5] E. Bompard, T. Huang, Y. Wu, M. Cremenescu, “Classification and trend analysis of threats origins to the security of power systems,” *International Journal of Electrical Power & Energy Systems*, Volume 50, September 2013, Pages 50-64, ISSN 0142-0615, http://dx.doi.org/10.1016/j.ijepes.2013.02.008.

[6] US Congress. Office of technology assessment, “Physical vulnerability of electric system to natural disasters and sabotage”, OTA-E-453 (Washington, DC: U.S. Government Printing Office; June 1990.

[7] S. Javier, W. Kevin, B. Ross, “Analysis of electric grid security under terrorist threat,” *IEEE Trans. Power System*, 2004:905–12.

[8] S. Halilcevic, F. Gubina, A. Gubina, “Prediction of power system security levels.” *IEEE Trans Power System*, 2009;24:368–77.

[9] T. Huang, S. L. Voronca, A. Purcarea, A. Estebsari, E. Bompard, “Analysis of chain of events in major historic power outages,” *Advances in Electrical and Computer Engineering*, *AECE*, 2014, Issue 3, ISSN: 1582-7445, e-ISSN: 1844-7600, doi: 10.4316/aece.

[10] Z. Qiong, J.W. Bialek, “Approximate model of European interconnected system as a benchmark system to study effects of cross-border trades,” *IEEE Trans. Power Systems*, vol.20, no.2, pp.782,788, May 2005

[11] E. Ciapessoni; D. Cirio; G. Kjølle; S. Massucco; A. Pitto; M. Sforna, "Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties," in IEEE Transactions on Smart Grid , in press, doi: 10.1109/TSG.2016.2519239

[12] Yang Liu, "Short-term operational reliability evaluation for power systems under extreme weather conditions," PowerTech, 2015 IEEE Eindhoven, Eindhoven, 2015, pp. 1-5. doi: 10.1109/PTC.2015.7232325

[13] M. Panteli; P. Mancarella, "Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events," in IEEE Systems Journal, in press, doi: 10.1109/JSYST.2015.2389272

[14] F. Dechesne, W. Pieters, Z. Lukszo, E. Bompard, T. Huang, A. Estebsari, J. Pascual, L. Lucena, J. Prieto, G. Higueras, A. Fuentes, P. Vaz Rebelo, S. Louise Voronca, M. Cremenescu, T. Ecatarina Roman, “D4.1 System Specification of Decision Support System”, Deliverable of the FP7 SESAME Project.

[15] E. Bompard, A. Estebsari, T. Huang, G. Fulli, “A framework for analyzing cascading failure in large interconnected power systems: A post-contingency evolution simulator,” International Journal of Electrical Power & Energy Systems, Volume 81, October 2016, Pages 12-21, ISSN 0142-0615, http://dx.doi.org/10.1016/j.ijepes.2016.02.010.

[16] A. Estebsari, E. Pons, T. Huang, E. Bompard, “Techno-economic impacts of automatic undervoltage load shedding under emergency,” Electric Power Systems Research, Volume 131, February 2016, Pages 168-177, ISSN 0378-7796, http://dx.doi.org/10.1016/j.epsr.2015.10.016.

[17] “KEY STATISTICS 2011, Energie-Control Austria, 2011”, Energie-Control Austria, [Available] http://www.e-control.at/en/publications/key-statistics